UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

TAHJAE FANIEL, individually and on behalf of all others similarly situated,	§	
	§	
Plaintiff,	§	
v.	§	**Case No. _____**
	§	
OAKBEND MEDICAL CENTER,	§	
	§	
*Defendan*t.	§	

CLASS ACTION COMPLAINT

Plaintiff Tahjae Faniel, individually and on behalf of all others similarly situated, bring this action against Defendant OakBend Medical Center ("OakBend" or "Defendant") a Texas Corporation. Plaintiff seeks to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") on Defendant's networks that resulted in unauthorized access to highly sensitive patient data.[1] As a result of the Data Breach, Plaintiff and 500,000 Class Members, [2] suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value

[1] Exhibit 1, ("Website Notice of Privacy Incident"), available at https://www.oakbendmedcenter.org/wp-content/uploads/2022/11/11-10-22-PDF-Website-Breach-Notice-Revised.pdf (last accessed Nov. 22, 2022).
[2] U.S. DHHS OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Nov. 20, 2022).

of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their sensitive personal information.

2. In addition, Plaintiff and Class Members' sensitive personal information—which was entrusted to Defendant, its officials, and its agents—was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes names, addresses, email addresses, date of birth, Social Security Numbers, ("PII"), and medical information ("PHI").[3] The PII and PHI that Defendant collected and maintained will be collectively referred to as the "Private Information."

4. Defendant OakBend Medical Center provides medical services in Houston and surrounding areas.[4] With over 50 locations and 1,200 employees, Defendant provides services to hundreds of thousands of patients annually.[5]

5. Plaintiff brings this class action lawsuit on behalf of herself and those similarly situated to address Defendant's inadequate safeguarding of her and Class Members' Private Information that Defendant collected and maintained, and for Defendant's failure to (1) provide timely and adequate notice to Plaintiff and other Class Members that their Private Information had been subject to the unauthorized access of an unknown third party, and (2) identify precisely what specific type of information was accessed.

6. Defendant maintained the Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on Defendant's computer system

[3] Exhibit 2, ("Faniel Notice Letter")
[4] Facts, OAKBEND MEDICAL CENTER, https://www.oakbendmedcenter.org/facts/ (last visited Nov. 21, 2022).
[5] *Id.*

and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. In addition, on information and belief, Defendant and its employees failed to properly monitor the computer network and IT systems that housed the Private Information.

8. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

9. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

11. Plaintiff and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. By this Complaint, Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

14. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence per se; (iii) breach of implied contract; (iv) unjust enrichment; (v) intrusion upon seclusion/invasion of privacy, and (vi) breach of fiduciary duty.

THE PARTIES

15. Plaintiff Tahjae Faniel is a natural person, resident, and a citizen of the State of Texas. She has no intention of moving to a different state in the immediate future. Plaintiff Faniel is acting on her own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Faniel's Private Information and owed him a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Faniel would not have entrusted her Private Information to Defendant had She known that Defendant failed to maintain adequate data security. Plaintiff Faniel's Private Information was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

16. Plaintiff received a notice letter from Defendant dated October 30, 2022, stating that on September 1, 2022, "we learned that cyber criminals had gained unauthorized access into various components of the OakBend Medical Center ("OakBend") computer network and that certain servers and computers were encrypted.."

17. Defendant OakBend Medical Center, LLC is a Texas corporation with a registered office in Fort Bend County–at 1705 Jackson St., Richmond, Texas 77469.

JURISDICTION AND VENUE

18. This Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

19. This Court has personal jurisdiction over the Defendant named in this action because Defendant is headquartered in this District and Defendant conducts substantial business in Texas and this District through its headquarters, offices, parents, and affiliates.

20. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

DEFENDANT'S BUSINESS

21. Defendant OakBend Medical Center provides medical services in Houston and surrounding areas.[6] With over 50 locations and 1,200 employees, Defendant provides services to hundreds of thousands of patients annually.[7]

[6] *Id.*
[7] *Id.*

22. On information and belief, in the ordinary course of medical care and medical billing, Defendant maintains the Private Information of patients and customers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Medication information;
- Health insurance information;
- Photo identification;
- Employment information, and;
- Other information that Defendant may deem necessary to provide care.

23. Additionally, Defendant may receive Private Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), close friends, and/or family Members.

24. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to patients, Defendant, upon information and belief, promises to, among other things: keep customers' PHI private; comply with healthcare industry standards related to data security and Private Information; inform customers and patients of legal duties and comply with all federal and state laws protecting customers' and patients' Private Information;

only use and release customers' Private Information for reasons that relate to medical care and treatment; and provide adequate notice to customers if their Private Information is disclosed without authorization.

25. As a condition of providing medical care Defendant requires that its customers entrust it with Private Information.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

27. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

28. Plaintiff and the Class had a reasonable expectation that Defendant would protect the Sensitive Information provided to and created by it, especially because, given the publicity of other data breaches and the significant impact they had, Defendant knew or should have known that failing to adequately protect patient information could cause substantial harm.

29. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information.

30. As described throughout this Complaint, Defendant did not reasonably protect, secure, or store Plaintiff's and the Class's Sensitive Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Defendant maintained.

Consequently, cybercriminals circumvented Defendant's security measures, resulting in a significant data breach.

THE CYBERATTACK AND DATA BREACH

31. Some date prior to September 1, 2022, one or more malicious actors gained access to Defendant's computer network and systems.[8] The actor(s) had access to Defendant's computer network and systems for an unknown amount of time. (the "Data Breach").

32. On September 1, 2022, Defendant became aware of the Data Breach when "cyber criminals gained unauthorized access into various components of the OakBend Medical Center ("OakBend") computer network and that certain servers and computers were encrypted."[9] In response, Defendant "took action to remediate this incident and hardened our system against future attacks."[10]

33. The investigation found the Data Breach resulted in the malicious actor(s) copying and exfiltrating substantial amounts of patient PII and PHI.[11] (collectively "Private Information") Specifically, the malicious actor(s) took files containing patient names, addresses, email addresses, date of birth, Social Security Numbers, and medical information.[12]

34. On or about October 28, 2022, Defendant ultimately admitted to the Data Breach and publicly acknowledged the data security incident to the United States Department of Health and Human Services' Office for Civil Rights ("DHHS").[13] On October 30, 2022, Defendant began

[8] Ex. 1.
[9] *Id.*
[10] *Id.*
[11] Ex. 2.
[12] *Id.*
[13] U.S. DHHS OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Nov. 20, 2022).

notifying the 500,000 impacted individuals, including Plaintiff and members of the proposed Class.[14] In its Notice, Defendant admitted that:

> On September 1, 2022, we learned that cyber criminals had gained unauthorized access into various components of the OakBend Medical Center ("OakBend") computer network and that certain servers and computers were encrypted. Immediately upon learning about this access and encryption, on the morning of September 1, 2022, we took action to remediate this incident and harden our system against future attacks.
>
> While we know that the cybercriminals had sufficient access to OakBend's systems to encrypt our data, our investigation indicates that a limited amount of data was actually transferred out of the OakBend computing environment. For example, we do not believe that the cybercriminals were able to remove the entire medical record of OakBend's patients. It does appear, however, that the cybercriminals were able to access and/or remove certain employee data sets and certain reports that included the personal and medical information related to our current and former patients, employees, and related individuals. In some instances, this information may have included the name, contact information (such as street and email address), social security number, and date of birth for the impacted individuals.[15]

35. Defendant identified only the following actions it undertook to mitigate and remediate the harm caused by the Data Breach in its Notice Letter:

> We conducted a thorough review of the incident, and our IT team has worked diligently to restore the integrity of our network.
>
> Furthermore, we have implemented additional security measures designed to prevent a recurrence pf such an attack and to protect the privacy of our patients, employees, and community members.[16]

36. Upon information and belief, and based on the type of cyberattack, along with public news reports, it is plausible and likely that Plaintiff's Private Information was stolen in the Data Breach. Plaintiff further believes her Private Information was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of all cybercriminals.

[14] *Id.*
[15] Ex. 1.
[16] Ex. 2.

37. Defendant had obligations created by HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

38. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

39. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

40. In light of recent high profile data breaches at other healthcare partner and provider companies, Defendant knew or should have known that its electronic records and patient and customer Private Information would be targeted by cybercriminals and ransomware attack groups.

41. Indeed, cyberattacks on medical systems like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[17]

42. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[18]

---

[17] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited June 23, 2021).

[18] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

43. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

44. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry and the prevalence of health care data breaches, Defendant inexplicably failed to adopt sufficient data security processes.

Defendant Failed to Comply with FTC Guidelines

45. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

46. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[19] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[20]

47. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords

[19] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 19, 2022).
[20] *Id.*

to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp,* 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

50. Defendant failed to properly implement basic data security practices.

51. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

52. Defendant was at all times fully aware of the obligation to protect the Private Information of customers and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

53. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Private

Information which they collect and maintain.

54. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

55. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

56. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

57. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

58. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

59. Covered entities must implement safeguards to ensure the confidentiality, integrity,

and availability of PHI. Safeguards must include physical, technical, and administrative components.

60. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

61. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40

62. The Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S BREACH

63. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to detect unauthorized ingress into its systems;

f. Failing to implement and monitor reasonable network segmentation to detect unauthorized travel within its systems, including to and from areas containing the most sensitive data;

g. Failing to detect unauthorized exfiltration of the most sensitive data on its systems;

h. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

i. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

j. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

k. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

l. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

m. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

n. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

o. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

p. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

q. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

r. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

s. Failing to adhere to industry standards for cybersecurity as discussed above; and

t. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

64. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

65. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

66. Cyberattacks and data breaches at healthcare companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

67. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[21]

68. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient

[21] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

outcomes, generally.[22]

69. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[23]

70. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

71. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone

[22] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.
[23] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[24]

72. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

73. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

74. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[25]

75. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

76. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance

[24] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 19, 2022).
[25] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[26]

77. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

78. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

79. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

80. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

81. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

---

[26] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Jan. 19, 2022).

82. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

83. Private Information can sell for as much as $363 per record according to the Infosec Institute.[27] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

84. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[28] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[29] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

85. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

86. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security

[27] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[28] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (Jan. 19, 2022).
[29] *Id* at 4.

number."[30]

87. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[31]

88. Medical information is especially valuable to identity thieves.

89. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[32] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[33]

90. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

91. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

92. To date, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the injury and damages they have suffered as a result of the Data Breach.

---

[30] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[31] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[32] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/.

[33] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

93. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

94. Plaintiff's name, address, date of birth, address, email address, Social Security. Number, and medical information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer systems.

95. Since being notified of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

96. Due to the Data Breach, Plaintiff anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring her accounts for fraudulent activity.

97. Plaintiff's Private Information was compromised as a direct and proximate result of the Data Breach.

98. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

99. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

100. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

101. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members. Plaintiff has already experienced various phishing attempts by telephone and through electronic mail.

102. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

103. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

104. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of its computer system and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for and agreed to.

105. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their medical accounts and sensitive information for misuse.

106. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

107. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

108. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

109. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Plaintiff's Experience

110. Plaintiff Faniel received medical care from OakBend in the past and is still a patient of OakBend. Upon information and belief, She was presented with standard medical forms to complete prior to her service that requested her PII and PHI, including HIPAA and privacy disclosure forms.

111. As part of her care and treatment, and as a requirement to receive Defendant's services, Plaintiff Faniel entrusted her Private Information to Defendant with the reasonable expectation and understanding that Defendant would take at a minimum, industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to the same. Plaintiff would not have used Defendant's services had She known that Defendant would not take reasonable steps to safeguard her Private Information.

112. In November 2022, Plaintiff Faniel received a letter from OakBend, dated October 30, 2022, notifying him that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. The notice indicated that Plaintiff Faniel's Private Information, including her name, address, email address, date of birth, Social Security number, and medical information was compromised as a result of the Data Breach.

113. As a result of the Data Breach, Plaintiff Faniel made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach and reviewing credit card and financial account statements.

She also intends to order a copy of her credit report and reach out to her insurance company to review those records as well to ensure that She has not been subject to any fraud. She is also in the process of changing passwords. She is also researching credit monitoring services to find an affordable option.

114. Plaintiff Faniel has spent multiple hours and will continue to spend valuable time She otherwise would have spent on other activities, including but not limited to work and/or recreation, to mitigate against the attempted fraud and against any future identity theft and fraud. As a direct and proximate result of the Data Breach, in October 2022, Plaintiff Faniel was notified by her bank that an unknown third party made fraudulent purchases on her debit card amounting to over $1,000 in charges. In addition, following the Data Breach, She experienced a substantial number of spam emails, texts messages, and phone calls.

115. Plaintiff Faniel is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Furthermore, Plaintiff Faniel stores any documents containing her sensitive information in a safe and secure location or destroys the documents. Moreover, She diligently chooses unique usernames and passwords for her various online accounts. Finally, Plaintiff Faniel has never previously had her identity stolen.

116. Plaintiff Faniel suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) actual fraud and identity theft; (b) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Faniel; (c) violation of her privacy rights; (d) the likely theft of her Private Information; and (e) imminent and impending injury arising from the increased risk of identity theft and fraud.

117. As a result of the Data Breach, Plaintiff Faniel has also suffered emotional distress as a result of the release of her Private Information, which She believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Faniel is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff also has suffered anxiety about unauthorized parties viewing, using, and/or publishing of information related to her medical records and prescriptions.

CLASS ACTION ALLEGATIONS

118. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class").

119. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All individuals residing in the United States whose PII and/or PHI was actually or potentially compromised during the period of unauthorized access to Defendant's computer systems as referenced in the Notice of Data Privacy Incident Defendant sent to Plaintiff and other Class Members on or around October 30, 2022 (the "Class").**

120. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

121. Plaintiff reserves the right to amend or modify the Class or Subclass definitions as this case progresses.

122. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists hundreds of thousands of individuals, including at least 500,000 individuals who were patients of Defendant whose sensitive data was compromised in Data Breach.

123. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached the duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts with Plaintiff and Class Members;

l. Whether Defendant were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

124. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

125. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

126. Predominance. Defendant have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from

Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

127. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

128. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

129. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely and adequately notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

130. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Class)

131. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

132. Defendant required customers, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of healthcare services.

133. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a

breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

134. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

135. Plaintiff and the Class are a well-defined, foreseeable, and probable group of patients that Defendant was aware, or should have been aware, could be injured by inadequate data security measures.

136. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Defendant knew or should have known that, given its repository of a host of Private Information for hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Defendant had a duty to reasonably safeguard its patients' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiff and the Class of inadequate data security created a duty to act reasonably and safeguard the Private Information.

137. Defendant's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Defendant and patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

138. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or

disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

139. In addition, Defendant has a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

140. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

141. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant includes, but is not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

142. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

143. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

144. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

145. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

146. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

147. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant has a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

148. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et seq.*, Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

149. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

150. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

151. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

152. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

153. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

154. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

THIRD COUNT
Breach of Implied Contract
(On behalf of the Plaintiff and the Class)

155. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

156. Plaintiff and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

157. Plaintiff and the Class were required to and delivered their Private Information to Defendant as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

158. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

159. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services or Plaintiff and Class Members.

160. In accepting such information and payment for services, Plaintiff and the other Class Members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

161. In delivering their Private Information to Defendant and paying for healthcare services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the data as part of that service.

162. Upon information and belief, in its written policies, Defendant expressly and impliedly promised to Plaintiff and Class Members that they would only disclose protected

information and other Private Information under certain circumstances, none of which related to a Data Breach as occurred in this matter.

163. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

164. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

165. Plaintiff and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

166. Had Defendant disclosed to Plaintiff and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their Sensitive Information to Defendant.

167. Defendant recognized that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

168. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendant.

169. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

170. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

FOURTH COUNT
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

171. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

172. This count is pleaded in the alternative to Count 3 (breach of implied contract).

173. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

174. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

175. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

176. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

177. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of rendering medical services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' Personal Information, and by providing Defendant with their valuable Personal Information.

178. Defendant was enriched by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

179. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

180. Defendant acquired the monetary benefit and Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

181. If Plaintiff and Class Members knew that Defendant had not secured their Personal Information, they would not have agreed to provide their Personal Information to Defendant.

182. Plaintiff and Class Members have no adequate remedy at law.

183. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

184. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

185. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FIFTH COUNT
Intrusion Upon Seclusion/Invasion of Privacy
(On Behalf of Plaintiff and the Class)

186. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

187. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.
>
> Restatement (Second) of Torts§ 652B (1977).

188. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

189. Defendant's conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion under common law.

190. By intentionally failing to keep Plaintiff's and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

191. Defendant knew that an ordinary person in Plaintiff's or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

192. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

193. Defendant intentionally concealed from and delayed reporting to Plaintiff and Class Members a security incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

194. The conduct described above was at or directed at Plaintiff and the Class Members.

195. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

196. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of himself and the Class.

SIXTH COUNT
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

197. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

198. In light of the special relationship between Defendant and Plaintiff and Class Members, Defendant became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant do store.

199. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with its patients, in particular, to keep secure their Private Information.

200. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period.

201. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

202. Defendant breached its fiduciary duty owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

203. Defendant breached its fiduciary duty to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

204. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

205. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and her counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and

Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and,

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: November 23, 2022

/s/ Ryan L. Thompson

Ryan L. Thompson, Attorney-In-Charge
Texas Bar No. 24046969
Southern District of Texas Bar No. 602642
Thompson Law LLP
3300 Oak Lawn Ave., 3rd Floor

Dallas, TX 75219
Telephone: (214) 755-7777
Facsimile: (214) 716-0116
rthompson@triallawyers.com

Brian C. Gudmundson**
Jason P. Johnston*
Michael J. Laird*
Rachel K. Tack*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
jason.johnston@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Christopher D. Jennings*
Nathan I. Reiter III
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300
Little Rock, AR 72201
Tel: (501) 372-1300
chris@yourattorney.com
nathan@yourattorney.com

* To be admitted *pro hac vice*
** To assume role of Attorney-In-Charge upon admission *pro hac vice*
Counsel for Plaintiff and the Proposed Class